Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Структурное подразделение «Институт информационных технологий и анализа данных»

УТВЕРЖДЕНА:
на заседании Совета института ИТиАД им. Е.И.Попова
Протокол №8 от 24 февраля 2025 г.

Рабочая программа дисциплины

«ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ»

Направление: 10.04.01 Информационная безопасность

Безопасность киберфизических систем

Квалификация: Магистр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Маринов Александр Андреевич Дата подписания: 22.06.2025	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 23.06.2025	Документ подписан простой электронной подписью Согласовал: Маринов Александр Андреевич Дата подписания: 22.06.2025

Год набора – 2025

Иркутск, 2025 г.

1 Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

1.1 Дисциплина «Технологии обеспечения информационной безопасности объектов» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ПК-5 Способность принимать участие в разработке систем обеспечения информационной безопасности или информационно-аналитических систем безопасности	ПК-5.1

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ПК-5.1	Осуществляет системный анализ прикладной области с целью выявления угроз и оценки уязвимости информационных систем	**Знать** методы подготовки рекомендаций руководству о правомерной защите от противоправных посягательств на объектах информатизации, а также систему подбора и обоснования технологий обеспечения информационной безопасности в зависимости от характера объекта информатизации. **Уметь** системно получать, анализировать и накапливать информацию с элементами прогнозирования по вопросам, относящимся к безопасности объекта; выбирать способы решения прикладных проблем информационной безопасности; прогнозировать основные опасности и угрозы, возникающие в процессе информационного взаимодействия. **Владеть** системным анализом прикладной области с целью выявления угроз и оценки уязвимости информационных систем в условиях становления современного информационного общества.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Технологии обеспечения информационной безопасности объектов» базируется на результатах освоения следующих дисциплин/практик: «Обработка и анализ научной информации»

Дисциплина является предшествующей для дисциплин/практик: «Производственная практика: эксплуатационная практика», «Технология создания защищенных киберфизических систем»

3 Объем дисциплины

Объем дисциплины составляет – 5 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 1
Общая трудоемкость дисциплины	180	180
Аудиторные занятия, в том числе:	104	104
лекции	52	52
лабораторные работы	0	0
практические/семинарские занятия	52	52
Самостоятельная работа (в т.ч. курсовое проектирование)	40	40
Трудоемкость промежуточной аттестации	36	36
Вид промежуточной аттестации (итогового контроля по дисциплине)	Экзамен	Экзамен

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 1

№ п/п	**Наименование раздела и темы дисциплины**	**Виды контактной работы**						СРС		**Форма текущего контроля**
		Лекции		ЛР		ПЗ(СЕМ)				
		№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	
1	2	3	4	5	6	7	8	9	10	11
1	Базовые сведения о межсетевых экранах	1	6			1	6	2	5	Устный опрос
2	Примеры межсетевых экранов	2	6			2	6	1	5	Устный опрос
3	Базовые сведения о VPN	3	6			3	6	2	5	Устный опрос
4	Туннелирование	4	7			4	7	1	5	Устный опрос
5	Протоколы создания VPN 2-го уровня модели OSI.	5	6			5	6	3	8	Устный опрос
6	Протоколы создания VPN 3-го уровня модели OSI	6	7			6	7	3	6	Устный опрос
7	Аудит и мониторинг ИБ в открытых	7	7			7	7			Доклад

	системах									
8	Защита от спама, другие средства защиты информации	8	7			8	7	3	6	Устный опрос
	Промежуточная аттестация								36	Экзамен
	Всего		52				52		76	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 1

№	Тема	Краткое содержание
1	Базовые сведения о межсетевых экранах	Назначение и функции МЭ. Основные компоненты МЭ. Принцип работы МЭ, варианты позиционирования МЭ. Руководящий документ Гостехкомиссии РФ по МЭ. Профили защиты для МЭ. Основные типы МЭ: экранирующие концентраторы, пакетные фильтры, шлюзы сеансового уровня, шлюзы прикладного уровня, МЭ экспертного уровня. Персональные МЭ. Основные компоненты МЭ. Слабости МЭ. Выбор реализаций МЭ.
2	Примеры межсетевых экранов	Маршрутизаторы, назначение и основные характеристики. Операционная система. Интерфейсы маршрутизаторов. Основные разделы и подразделы меню комплекса межсетевых экранов. Идентификация и аутентификация комплекса в сети. Удаленное администрирование, построение VPN на базе комплекса
3	Базовые сведения о VPN	Различные подходы к определению VPN, определение компании Check Point Software Technologies. Цели и задачи применения VPN-технологий. Преимущества VPN по сравнению с защищенными выделенными каналами связи и другими методами организации защищенной связи. Классификация VPN. Специфика построения VPN. Критерии, предъявляемые к VPN. Классификация VPN компании Check Point по типу устанавливаемых соединений: Intranet VPN, Client\Server VPN, Extranet VPN, Remote Access VPN – определения, характерные черты и особенности использования. Классификация VPN согласно консорциуму VPN (VPNC) по степени защищенности: доверенные, защищенные и смешанные VPN – определения, требования, технологии построения.
4	Туннелирование	Механизм туннелирования как основа построения VPN. Общий поход к созданию туннелей, функции конкретных протоколов, участвующих в процессе туннелирования. Обеспечение конфиденциальности, подлинности и целостности

		при использовании инкапсуляции данных. Базовая схема VPN. VPN-агенты. Функции VPN-агентов. Обработка входящих и исходящих пакетов. Различные варианты позиционирования и использования VPN-агентов.
5	Протоколы создания VPN 2-го уровня модели OSI.	Протокол PPTP. Функции протокола. Компоненты PPTP. Сценарии работы протокола. Архитектура PPTP. Управляющее соединение и управляющие сообщения. Инкапсуляция данных при передаче. Аутентификация, контроль доступа и шифрование. Настройка VPN на базе протокола PPTP в среде Windows.
6	Протоколы создания VPN 3-го уровня модели OSI	Архитектура IPSec. Функции, принцип работы, сценарии применения IPSec. Обзор основных компонентов IPSec. Главные базы данных IPSec: SPD, SAD, PAD. Политики безопасности IPSec. Ассоциации безопасности (SA): определение, назначение, процедуры управления. Обработка IP-трафика. Особенности обработки ICMP-трафика и фрагментированных IP-пакетов. Использование аудита в архитектуре IPSec. Защита данных с помощью протоколов AH и ESP. Инкапсуляция данных в транспортном и туннельном режимах работы. Форматы заголовков. Защищаемые поля IP-заголовка при использовании AH в транспортном режиме. Обработка исходящих (поиск SA, генерация порядкового номера, вычисление ICV и шифрование данных, фрагментация) и входящих (сборка, поиск SA, проверка порядкового номера, проверка ICV, расшифрование, проверка на соответствие записи в SPD) пакетов. Использование комбинированных криптографических алгоритмов в ESP. Особенности использования расширенных (64-битных) порядковых номеров. Защита от повторной передачи пакетов.
7	Аудит и мониторинг ИБ в открытых системах	Средства анализа защищенности (САЗ) и их место в защите открытых систем. Классификации САЗ. Сетевые сканеры: размещение агентов, принципы работы, этапы работы; сравнение современных реализаций. Системные сканеры. САЗ для приложений. Критерии выбора САЗ. Методы отражения вторжений: предотвращение, прерывание, сдерживание, отклонение, обнаружение, устранение последствий. Системы обнаружения/предотвращения вторжений (СОВ/СПВ). Классификация и структура СОВ/СПВ. Системные и сетевые СОВ/СПВ: принципы работы, достоинства и недостатки. Размещение сетевых СОВ/СПВ. Интеллектуальные и поведенческие СОВ.

		Обнаружение вторжений/злоупотреблений; обнаружение аномалий/сопоставление с образцом. СОВ, их выбор, применение, ограниченность и примеры систем. СПВ, их применение и примеры систем. Сохранение доказательств вторжений. Стандарты в области обнаружения вторжений.
8	Защита от спама, другие средства защиты информации	Защита от спама в электронной почте: определение, методы детектирования, архитектура защищенной от спама электронной почты, примеры систем. Многофункциональные устройства защиты от сетевых атак. Системы анализа и управления рисками. Системы обеспечения ИБ на уровне предприятия.

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 1

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Назначение и функции МЭ	6
2	Идентификация и аутентификация комплекса в сети	6
3	Классификация VPN	6
4	Механизм туннелирования как основа построения VPN	7
5	Протоколы создания VPN	6
6	Протоколы создания VPN 3-го уровня модели OSI	7
7	Аудит и мониторинг ИБ в открытых системах	7
8	Защита от спама, другие средства защиты информации	7

4.5 Самостоятельная работа

Семестр № 1

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям	10
2	Подготовка презентаций	10
3	Решение специальных задач	20

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: В ходе проведения лекций, практических работ используются следующие интерактивные методы обучения: в теоретическом курсе предусматривается проведение интерактивной лекции по темам: «Протоколы создания VPN», «Аудит и мониторинг ИБ в открытых системах», «Защита от спама, другие средства защиты

информации» (Темы №6,7,8); при проведении практических работ предусматривается решение задач по расчетам итоговых показателей, а также проведение при решении задач по индивидуальным заданиям «разбора конкретных ситуаций».

5 Перечень учебно-методического обеспечения дисциплины

5.1 Методические указания для обучающихся по освоению дисциплины

5.1.1 Методические указания для обучающихся по практическим занятиям

https://el.istu.edu/mod/book/edit.php?cmid=326915

5.1.2 Методические указания для обучающихся по самостоятельной работе:

https://el.istu.edu/mod/folder/view.php?id=326916&forceview=1

6 Фонд оценочных средств для контроля текущей успеваемости и проведения промежуточной аттестации по дисциплине

6.1 Оценочные средства для проведения текущего контроля

6.1.1 семестр 1 | Устный опрос

Описание процедуры.

Устный опрос проводится по окончанию лекционных занятий путем опроса студентов по списочному составу (при наличии бюджета времени после обсуждения установленных вопросов).

Критерии оценивания.

ответы на поставленные вопросы; допускается помощь в ответах со стороны аудитории (давшие правильный ответ освобождаются от персональной очереди отвечающих по списку).

6.1.2 семестр 1 | Доклад

Описание процедуры.

Доклад по длительности занимает 10-12 минут (выступление длится около 7-8 минут) остальное время ответы на вопросы по докладу. В процессе подготовки доклада или выступления обучающимся используются самостоятельная работа и консультации преподавателя. Доклад должны быть логически хорошо построены, раскрывать рассматриваемый вопрос или проблему, давать полезные сведения аудитории

Критерии оценивания.

Отлично: студентом задание решено самостоятельно. При этом составлен правильный алгоритм решения задания, в логических рассуждениях, в выборе формул и решении нет ошибок, получен верный ответ, задание решено рациональным способом.
Хорошо: студентом задание решено с подсказкой преподавателя. При этом составлен правильный алгоритм решения задания, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор формул для решения; есть объяснение решения, но задание решено нерациональным способом или допущено не более двух несущественных ошибок, получен верный ответ.

Удовлетворительно: обучающимся подготовлен доклад с подсказками преподавателя. При этом доклад понятен и составлен правильно, в логическом рассуждении нет существенных ошибок, но допущены существенные ошибки в выборе (структуры, формул) или в математических расчетах; доклад подготовлен не полностью или в общем виде.
Неудовлетворительно: обучающийся не подготовил доклад

6.2 Оценочные средства для проведения промежуточной аттестации

6.2.1 Критерии и средства (методы) оценивания индикаторов достижения компетенции в рамках промежуточной аттестации

Индикатор достижения компетенции	Критерии оценивания	Средства (методы) оценивания промежуточной аттестации
ПК-5.1	Способен применять современные средства поиска ин-формации в вопросах при-кладной области. Способен анализировать связи выявлять угрозы уязвимости ин-формационных систем.	Устное собеседование по теоретическим вопросам и/или выполнение практических заданий

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 1, Типовые оценочные средства для проведения экзамена по дисциплине

6.2.2.1.1 Описание процедуры

1) Экзамен по дисциплине проводится согласно расписанию в назначенной аудитории, в которую приглашается к установленному началу экзамена группа студентов.
2) К экзамену допускаются студенты, которые выполнили все предусмотренные работы по освоению курса: сданы практические работы по выбранной теме.
3) Каждый студент из числа допущенных выбирает один билет и готовится к ответу в течение не менее 30 - 45 минут письменно на поставленные два вопроса в билете.

Пример задания:

Экзамен проводится в форме устного опроса по экзаменационным билетам.
1. Требования информационной безопасности.
2. Зависимость требований от структуры объектов информатизации.
3. Технологии формирования алгоритмов обработки информации.
4. Информационно-коммуникационные технологии в фундаментальных проблемах информационной безопасности.
5. Информационно-коммуникационные технологии для выявления и анализа информационной безопасности.
6. Проблемы информационной безопасности в условиях становления современного информационного общества.

7. Специфика технологий обеспечения информационной безопасности объектов защиты.
8. Требования к технологиям обеспечения информационной безопасности объектов защиты.
9. Методы анализа информационной системы для выбора технологий обеспечения информационной безопасности.
10. Информационная безопасность объектов информатизации.
11. Современные технологии защиты объектов информатизации.
12. Методы отражения вторжений: предотвращение, прерывание, сдерживание, отклонение, обнаружение, устранение последствий.
13. Особенности обработки ICMP-трафика и фрагментированных IP-пакетов.
14. Настройка VPN на базе протокола PPTP в среде Windows.
15. Классификация VPN компании Check Point по типу устанавливаемых соединений.
16. Защита данных с помощью протоколов AH и ESP.
17. Обеспечение конфиденциальности, подлинности и целостности при использовании инкапсуляции данных.
18. Базовая схема VPN, VPN-агенты, функции VPN-агентов.
19. Подбор и обоснование технологий обеспечения информационной безопасности в зависимости от характера объекта информатизации.
20. Технологии для формирования проектных решений по защите объектов информатизации.

6.2.2.1.2 Критерии оценивания

Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
Уверенно и без ошибок отвечает на все вопросы билета	Допускает незначительные ошибки в ответе на один из вопросов, включая дополнительные по результатам собеседования	Знает ответы на два вопроса или допускает ошибки в ответах на вопросы	Не отвечает на два и более вопросов

7 Основная учебная литература

1. Попова Е. С. Информационная безопасность и защита информации [Электронный ресурс] : курс лекций / Е. С. Попова, 2009. - 68.

2. Хорев П. Б. Программно-аппаратная защита информации : учебное пособие для вузов по направлениям "Информационная безопасность" и "Информатика и вычислительная техника" / П. Б. Хорев, 2012. - 351.

8 Дополнительная учебная литература и справочная

1. Карлинг М. Системное администрирование Linux: Пер. с англ. / М. Карлинг, Стефен Деглер, Джеймс Деннис, 2000. - 319.

2. Глухих В. И. Информационная безопасность и защита данных : учебное пособие / В. И. Глухих, 2012. - 244.

3. Митчелл Марк. Программирование для Linux: Проф. подход : [Пер. с англ.] / Марк Митчелл, Джеффри Оулдем, Алекс Самьюэл, 2002. - 287.

4. Манн Скотт. Безопасность Linux: Рук. администратора по системам защиты с открытым исход. кодом : [Пер. с англ.] / Скотт Манн, Эллен Митчелл, Митчелл Крелл, 2003. - 621.

5. Собелл М. Г. Практическое руководство по Red Hat® Linux® : Fedora™ Core и Red Hat Enterprise Linux : пер. с англ. / Марк Г. Собелл, 2005. - 1071.

6. Петерсон Ричард. Linux: руководство по операционным системам / Ричард Петерсон; Пер. с англ. С. М. Тимачева, 1997. - 687.

7. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации : учеб. пособие для вузов по специальности 075400 "Комплекс. защита объектов информ." / А. А. Малюк, 2004. - 280.

9 Ресурсы сети Интернет

1. http://library.istu.edu/
2. https://e.lanbook.com/

10 Профессиональные базы данных

1. http://new.fips.ru/
2. http://www1.fips.ru/

11 Перечень информационных технологий, лицензионных и свободно распространяемых специализированных программных средств, информационных справочных систем

1. Свободно распространяемое программное обеспечение Microsoft Windows Seven Professional (Microsoft Windows Seven Starter) - Seven, Vista, XP_prof_64, XP_prof_32 - поставка 2010

2. Свободно распространяемое программное обеспечение Microsoft Windows Seven Professional [1x100] RUS (проведен апгрейд с Microsoft Windows Seven Starter [1x100]) - поставка 2010

3. Свободно распространяемое программное обеспечение Microsoft Windows Server Standard 2008 R2 Russian Academic OPEN 1 License No Level

12 Материально-техническое обеспечение дисциплины

1. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

2. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

3. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

4. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

5. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

6. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

7. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

8. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

9. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

10. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

11. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

12. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

13. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

14. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

15. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО

16. Рабочая станция: ASUS P5Q-EM/Intel Core 2 Duo E8500/DDRII DIMM 2Gb/320 Gb/DVD-RW/512Mb PCI-E GF/мон.19" LG/блок ИБП/мышь/кл+ ПО